

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MISSOURI  
WESTERN DIVISION**

DANIEL ARNOLD individually, and on  
behalf of all other similarly situated,

Plaintiff,

v.

JOHN FITZGIBBON MEMORIAL  
HOSPITAL, INC. d/b/a FITZGIBBON  
HOSPITAL, a Missouri nonprofit  
corporation,

Defendant.

Case No.:

**CLASS ACTION COMPLAINT  
JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Daniel Arnold (“Plaintiff”), individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant John Fitzgibbon Memorial Hospital, Inc. d/b/a Fitzgibbon Hospital (“Fitzgibbon” or “Defendant”), based upon personal knowledge as to themselves, their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

**NATURE OF THE ACTION**

1. In or around June of 2022, Defendant Fitzgibbon experienced a data breach whereby its internal systems were infiltrated by a ransomware attack. As a result of that data breach, unauthorized third-party hackers acquired the personal identifying information (“PII”) and protected health information (“PHI”) of approximately 112,072 of Fitzgibbon’s patients. This information included, *inter alia*, the names, Social Security numbers, driver’s license numbers, financial account numbers, health insurance information, and/or medical information of those patients.

2. According to its website, Defendant is a “leader in central Missouri in providing quality, compassionate care and personal attention to our patients.”<sup>1</sup> As a requirement to obtain its services, Defendant collects and stores its patients’ it with their PII and PHI in its internal data servers.

3. Under statute and regulation, Defendant had a duty to implement reasonable and adequate industry-standard data security policies and safeguards to protect the PII and PHI entrusted to it by its patients. However, Defendant failed to implement such security policies and safeguards and allowed third-party hackers to exfiltrate its patients’ PII and PHI.

4. Plaintiff and Class Members have suffered injuries and damages. As a result of Defendant’s wrongful actions and inactions, Plaintiff and Class Members have suffered injuries and damages. Plaintiff and Class Members’ sensitive PII and PHI—including their driver’s license numbers, financial account information and Social Security numbers—have been compromised. Plaintiff and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit and medical fraud for the remainder of their lifetimes. Plaintiff and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts, and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiff and Class Members have also lost the value of their PII and PHI.

5. Further, Defendant unreasonably delayed in notifying Plaintiff and Class Members of the data breach until approximately January 5, 2023—despite having discovered the breach as early as June 21, 2022, over six months earlier. Even more egregiously, Defendants’ data breach notification makes false statements regarding Defendants’ discovery of the breach.

---

<sup>1</sup> <https://www.fitzgibbon.org/>.

6. As a result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have had their PII and PHI compromised and stolen by nefarious third-party hackers, have had their privacy rights violated, have been exposed an increased risk of fraud and identity theft, and have otherwise suffered damages. Plaintiff and Class Members bring this action to seek redress against Defendant.

### **PARTIES**

7. Plaintiff Daniel Arnold is a citizen Saline, Missouri.

8. Defendant John Fitzgibbon Memorial Hospital, Inc. d/b/a Fitzgibbon Hospital is a Missouri nonprofit corporation with its principal place of business located at 2305 S Highway 65, P.O. Box 250, Marshall, Missouri 65340-3702.

### **JURISDICTION AND VENUE**

9. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), as the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and there are numerous Class Members who are citizens of states other than Defendant's state of citizenship.

10. This Court also has personal jurisdiction over the Parties because Defendant resides in and routinely conducts business in this State and has sufficient minimum contacts in this State to have intentionally availed themselves to this jurisdiction.

11. Venue is proper in this District because, among other things: (a) Plaintiff Daniel Arnold resides in this District, (b) Defendant resides in and conducts substantial business in this District; (c) Defendant directed its services at residents in this District, and (d) many of the acts and omissions that gave rise to this action took place in this District.

## **FACTUAL BACKGROUND**

### **A. The Data Breach**

12. Defendant Fitzgibbons is a HIPAA healthcare provider that provides a wide variety of medical services to patients throughout the central Missouri area. In providing these services, Defendant requires that its patients provide it with their sensitive PII and PHI, which it aggregates and stores within its internal data systems. As a result, Defendant's internal systems store the PII and PHI of hundreds of thousands of Missouri residents who have used its services.

13. In June of 2022, Defendant's systems were targeted by hacker group DAIXIN Team in a ransomware attack, who obtained and exfiltrated approximately 40GB of data from Defendant's internal data servers.<sup>2</sup> This data included, *inter alia*, database tables from Defendant's MEDITECH database and sensitive documents containing patient PII and PHI. Notably, two files published in this beach found to contain patient PII/PHI were .csv files with 750,000 rows and over one million rows of data respectively—indicating that the total number of affected individuals may be far greater than reported by Defendant.<sup>3</sup>

14. The DAIXIN Team promptly made that stolen data available for public download on the dark web and included with that data a list of crimes that an individual could commit with another person's PII/PHI.<sup>4</sup>

---

<sup>2</sup> "Fitzgibbon Hospital, Diskriter, Christiana Spine Center Suffer Ransomware Attacks" <https://www.hipaajournal.com/fitzgibbon-hospital-diskriter-christiana-spine-center-suffer-ransomware-attacks/> (last accessed January 16, 2023).

<sup>3</sup> "MO: Fitzgibbon Hospital hit by ransomware, sensitive data leaked." <https://www.databreaches.net/mo-fitzgibbon-hospital-hit-by-ransomware-sensitive-data-leaked/> (last accessed January 16, 2023).


<sup>4</sup> "MO: Fitzgibbon Hospital hit by ransomware, sensitive data leaked." <https://www.databreaches.net/mo-fitzgibbon-hospital-hit-by-ransomware-sensitive-data-leaked/> (last accessed January 16, 2023).

Figure 1  
Patient PII/PHI Posted on the Dark Web

# DAIXIN Team

Here you can get links to:

Information compromised in the Data Breach includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, 'PII'), and medical and treatment information ('PHI'), The PII and PHI that collected and maintained - the 'Private Information.' Private Information can commit a variety of crimes including, e.g., opening new financial accounts, taking out loans in, using to obtain medical services, using health information to target other phishing and hacking intrusions based on their individual health needs, using information to obtain government benefits, filing fraudulent tax returns using information, obtaining driver's licenses in names but with another person's photograph, and giving false information to police during an arrest.



## Fitzgibbon Hospital (USA)

Web Site: <https://www.fitzgibbon.org>

Fitzgibbon Hospital is a leader in central Missouri in providing quality, compassionate care and personal attention to patients.

---

STOLEN DATA INCLUDES: Database tables dump from MEDITECH DB, Sensitive documents from internal servers (40 GB) [fileslist.zip](#)

Leak 1 : [Meditech table LabRequisitionDetails.csv.zip](#)

Leak 2 : [Meditech table BarInsurances.csv.zip](#)

Leak 3 : [Meditech table ABSInsurance.csv.zip](#)

Leak 4 : [Table MmStockReqs.csv.zip](#)

Leak 5 : [Directory "Converted toPDF/"](#) (emails in PDF)

Leak 6 : [Directory "Cancer Center Forms/SCANNED DOCUMENTS/"](#) (Have PII PHI)

===== [FULL LEAK](#) =====

15. In addition to files containing patient PII/PHI, the data posted by DAIXIN contained a number of files relating to Defendant's cybersecurity safeguards, including a report detailing the results of a cybersecurity assessment the hospital had conducted in 2019. This report was viewable, despite being password protected, because the password for the files was stored in the same folder as the would-be protected report.<sup>5</sup> As a result, Defendant's cybersecurity protocols and procedures, including any known vulnerabilities therein, have now been made public—and thus ripe for further exploit. This blatant disregard for best practices is indicative of the lacking state of Defendants' cybersecurity safeguards that were in place at the time of the breach.

**B. Defendant's Unreasonable and Inadequate Data Security**

16. Plaintiff and Class Members provided their sensitive PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would implement reasonable and adequate cybersecurity safeguards to protect their PII and PHI from unauthorized disclosure. What Plaintiff and Class Members did not expect was that Defendant would cause their sensitive PII and PHI to be obtained by unauthorized third parties by leaving itself vulnerable to a ransomware attack.

17. Ransomware is a form of malware designed to gain unauthorized access to and encrypt files on a device or server, rendering any files and the systems that rely on them unusable. Malicious actors use ransomware to unlawfully obtain private, sensitive and/or confidential information, and then demand a ransom in exchange for decrypting the affected files. Ransomware attacks are often targeted towards businesses such as Defendant that are known to collect and store the confidential and sensitive PII/PHI of hundreds of thousands of individuals.

---

<sup>5</sup> *Id.*

18. Ransomware attacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards and/or proper employee cybersecurity training, as the vast majority of ransomware incidents are caused by poor user practices, lack of cybersecurity training, and weak passwords or access management.<sup>6</sup> For instance, ransomware is most commonly spread through “phishing” emails sent to employees with customer or patient data on their devices, which contain malicious attachments that allow a hacker to access that patient data. Ransomware is also commonly spread when an employee visits an infected website on a device connected to a company server. As such, businesses with adequate and reasonable data security practices train their employees not to open email attachments from unrecognized emails or visit unauthorized websites on company device.

19. Defendant notes that it is “committed to protecting your health information” and that “[w]e are also required by law to protect the privacy of your protected health information” on its public-facing Notice of Privacy Practices.<sup>7</sup> Despite this, Defendant clearly failed to implement adequate and reasonable cybersecurity safeguards to protect Plaintiff and Class Members’ PII and PHI. This can clearly be inferred from, *inter alia*, Defendant’s failure to password protect certain data security files, as well as Defendant’s failure to adequately train its staff against avoidable phishing attacks.

---

<sup>6</sup> “Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020.” Statista, <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/> (last accessed January 16, 2023).

<sup>7</sup> “Notice of Privacy Practices,” [https://www.fitzgibbon.org/Content/Uploads/fitzgibbon.org/files/Privacy%20Notice%20\(18x24%20poster\)%201-2023.pdf](https://www.fitzgibbon.org/Content/Uploads/fitzgibbon.org/files/Privacy%20Notice%20(18x24%20poster)%201-2023.pdf) (last accessed January 16, 2023).



**C. Defendant's Unreasonably Delayed and Misleading Data Breach Notification**

20. Defendant owed Plaintiff and Class Members a duty under state law and federal law to provide timely notification of the data breach. The Missouri Data Breach Notification Statute provides that “any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery of notification of the breach.” Mo. Rev. Stat. §407.1500.2(1). §407.1500.2(1)(a) of that same statute states that such notification shall be “[m]ade without unreasonable delay.”

21. Likewise, 45 C.F.R. §164.404 of the Health Insurance Portability and Accountability Act (“HIPAA”) provides that a “covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.” As a healthcare provider, Defendant is a covered entity under HIPAA.

22. In its Data Breach Notice to its affected Patients, Defendant claims that, despite detecting the data breach on June 6, 2022, it “discovered on December 1, 2022 that some patients’ identifiable and/or protected health information may have been accessed and acquired.”<sup>8</sup> While this statement would seemingly put Defendant within a notification timeframe permissible under §407.1500 and 45 C.F.R. §164.404, the statement is false and misleading—as Defendant must have become aware that the data breach had affected patient PII/PHI in June of 2022.

23. The DAIXIN Team published Defendants’ stolen data, including patient PII/PHI, on the dark web in June of 2022. Defendant was contacted multiple times by at least one

---

<sup>8</sup> “Notice of Data Security Incident” <https://www.fitzgibbon.org/Content/Uploads/fitzgibbon.org/files/Notice%20of%20Data%20Security%20Incident.pdf> (last accessed January 16, 2023).



publication for comment regarding this breach, and thus must necessarily have become aware that patient PII/PHI had been stolen around this time.<sup>9</sup>

24. Furthermore, a spokesperson from the DAIXIN Team has since revealed chatlogs depicting a June 21, 2022 ransom demand conversation between the DAIXIN Team and Defendant:

**Fitzgibbon Hospital 2022-06-21 20:47:59:**

It looks like we have no choice but to agree to this amount. As long as there are no fees for payment in bitcoins then we can submit this for approval. It is not easy for us as there are multiple organizations we have to get approval from including our board of directors. If we have an agreement we can send payment by Friday. Agreed? If so please add three days to the timer and we will let you know when the approvals are completed.

**Admin 2022-06-21 20:54:10**

It looks like you're just stalling.

**Fitzgibbon Hospital 2022-06-21 20:56:44**

We are not. We promise. We were hoping you would take a lower amount because it would have been easier. But because of this larger sum we have to get different people to agree. We have limitations that we have to work through and get approved. It's more of a formality process now. It's possible Thursday we can send but want to be sure we have enough time without asking you again so we are asking until Friday.

**Admin 2022-06-21 21:04:03**

ok. If we have come to an agreement, then, as we promised, we give additional time for payment. Let it be on Friday. If there is no payment on Friday, the agreement is terminated with all the ensuing consequences.<sup>10</sup>

25. According that same DAIXIN Team spokesperson, Defendant was given a test decryption and shown proof of data exfiltration during the course of these ransom negotiations.<sup>11</sup> At this time, Defendant must have become aware that patient PII/PHI had been stolen as a part of the breach. Defendant cannot possibly claim that they did not discover that fact until December of 2022.

---

<sup>9</sup> "MO: Fitzgibbon Hospital hit by ransomware, sensitive data leaked." <https://www.databreaches.net/mo-fitzgibbon-hospital-hit-by-ransomware-sensitive-data-leaked/> (last accessed January 16, 2023).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

26. Defendant ultimately did not pay the ransom demanded by the DAIXIN TEAM, and the DAIXIN Team began publishing the stolen data on the dark web shortly thereafter.

27. Defendant's false and misleading statement as to when they discovered that the data breach had impacted patient PII/PHI is unconscionable. Further, as a result of Defendant's unreasonable delay, Plaintiff and Class Members were left unaware that their sensitive PII and PHI had been acquired by nefarious third-party hackers for over six months and were thus unreasonably delayed in their ability and opportunity to take emergency prophylactic measures to protect their personal and financial accounts.

**D. Defendant's Obligation to Protect Patient PII/PHI Under Federal Law**

28. As a HIPAA covered entity, Defendant holds a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Member's PII/PHI. Under the HIPAA Privacy Rule, Defendant is required to, *inter alia*:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives maintains or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance with the above data security procedures by their workforce.

45 CFR §164. 306(a)

29. The HIPAA Privacy Rule also requires Defendant to "review and modify the security measures implemented...as needed to continue provision of reasonable and appropriate

protection of electronic protected health information” under 45 C.F.R. §164.306(e) and to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights” under 45 C.F.R. §164.312(a)(1).

30. Further, the Federal Trade Commission Act, 15 U.S.C. §45 prohibits businesses such as Defendant from engaging in “unfair or deceptive acts or practices affecting commerce.” The Federal Trade Commission (“FTC”) has found that a company’s failure to maintain reasonable and appropriate data security for the consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

31. Defendant has failed to comply with each of these federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiff and Class Members’ PII/PHI.

**E. Defendant’s Failure to Comply with Industry Data Security Standards and Regulations**

32. Experts in the field of data security are in consensus that healthcare providers such as Defendant are specifically targeted by hackers due to the value of the PII/PHI that they collect and maintain as a part of their ordinary course of business. As such, experts have identified several best practices that healthcare providers such as Defendant should implement and follow in order to best protect themselves from unauthorized access.

33. Such best practices are outlined in the National Institute of Standards and Technology’s (“NIST”) “Security and Privacy Controls for Information Systems and Organizations” publication. These best practices include, *inter alia*, maintaining a plan of action

for preventing and addressing data breaches, training and educating employees on data security, implementing strong password requirements, implementing multi-layer security such as two-factor authentication, installation and maintenance of firewalls, anti-virus and anti-malware software, implementing data encryption, monitoring and protection of web browsers and email management systems, and limiting the number of employees with access privileges to patient PII/PHI. *See, e.g.*, NIST SP 800-53, Rev. 5 AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AT-1, AT-3, CA-1, CA-2, CA-3, CA-7, IA-1, IA-2, IA-3, PL-1, PL-2, PM-1, PT-1, PT-2, PT-3.

34. The FTC has also promulgated numerous guides for business which highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, “Protecting Personal Information: A Guide for Business,”<sup>12</sup> which establishes guidelines for fundamental data security principles and practices for business. Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach.<sup>13</sup> Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security;

---

<sup>12</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>. (last accessed January 16, 2023).

<sup>13</sup> *Id.*

monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>14</sup>

**F. Applicable Standards of Care**

35. In addition to their obligations under federal law and regulation, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and Class Members.

36. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their computer system to ensure that the PII/PHI in Defendants' possession was adequately secured and protected.

37. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in their possession, including adequately training their employees and others who accessed the PII/PHI in their possession, including adequately training their employees and others who accessed PII/PHI in their computer systems on how to adequately protect PII/PHI.

38. Defendant owed a duty of care to Plaintiff and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

---

<sup>14</sup> Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) <https://www.ftc.gov/business-guidance/resources/start-security-guide-business>. (last accessed January 16, 2023).

39. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

40. Defendant owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII/PHI to Defendant.

41. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

42. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant received PII/PHI from Plaintiff and Class Members with the understanding that Plaintiff and Class Members expected their PHI/PII to be protected from disclosure. Defendant knew that a breach of its data systems would cause Plaintiff and Class Members to incur damages.

**G. Stolen Information is Valuable to Hackers and Thieves**

43. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendant opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiff and Class Members.

44. Plaintiff and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

45. Legitimate organizations and criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

46. PII/PHI is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as “dumps.”<sup>15</sup>

47. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim’s digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim’s accounts, as well as from those belonging to family, friends, and colleagues.

48. In addition to PII/PHI, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.<sup>16</sup>

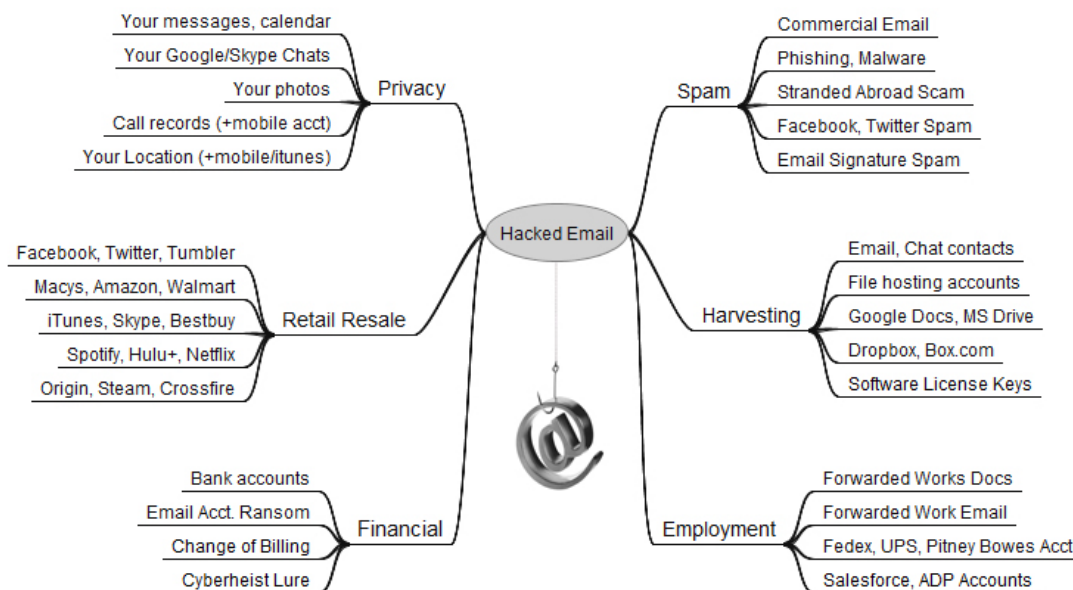
---

<sup>15</sup> See *All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/> (last accessed January 16, 2023).

<sup>16</sup> *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>. (last accessed January 16, 2023.)



49. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.<sup>17</sup>



50. Hacked information can also enable thieves to obtain other personal information through “phishing.” According to the Report on Phishing available on the United States, Department of Justice’s website: “AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.”<sup>18</sup>

<sup>17</sup> Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>. (last accessed January 16, 2023).

<sup>18</sup> *Report on Phishing* (Oct. 2006), [https://www.justice.gov/archive/opa/docs/report\\_on\\_phishing.pdf](https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf) (last accessed January 16, 2023).

## **H. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud**

51. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII/PHI of Plaintiff and the Class Members. The ramification of Defendant's failure to keep Plaintiff and the Class Members' data secure is severe.

52. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.<sup>19</sup> In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.<sup>20</sup> The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the "worst ever year" for healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.<sup>21</sup>

53. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."<sup>22</sup> In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id.*

---

<sup>19</sup> *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/>. (last accessed January 16, 2023).

<sup>20</sup> *December 2019 Healthcare Data Breach*, HIPAA Journal (Jan 21, 2020), <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed January 16, 2023).

<sup>21</sup> "Largest Healthcare Data Breaches of 2021," HIPAA Journal (Dec. 30, 2021), <https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/> (last accessed December 2, 2022).

<sup>22</sup> *See Victims of Identity Theft*, U.S. Department of Justice (September 2015, revised November 13, 2017), <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (last accessed December 2, 2022).

## **I. Annual Monetary Losses from Identity Theft are in the Billions of Dollars**

54. Javelin Strategy and Research reports that losses from identity theft reached \$21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), <http://www.gao.gov/new.items/d07737.pdf>. (last accessed January 16, 2022.)

55. This is particularly the case with HIPAA data breaches such as Defendant’s, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.<sup>23</sup> Victims of medical identity theft “often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”<sup>24</sup>

56. Indeed, a study by Experian found that the average total cost of medical identity theft is “nearly \$13,500” per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.<sup>25</sup> Victims of healthcare data breaches often find themselves

---

<sup>23</sup> Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), <https://khn.org/news/rise-of-identity-theft/>. (last accessed January 16, 2022).

<sup>24</sup> *Id.*

<sup>25</sup> *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>. (last accessed January 16, 2022).

“being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores.”<sup>26</sup>

57. Plaintiff and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

**J. Plaintiff and Class Members Suffered Damages**

58. The exposure of Plaintiff and Class Members’ PII/PHI to unauthorized third-party hackers was a direct and proximate result of Defendant’s failure to properly safeguard and protect Plaintiff and Class Members’ PII from unauthorized access, use, and disclosure, as required by and state and federal law. Upon information and belief, the data breach was also a result of Defendant’s failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class Members’ PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and federal statute and regulation.

59. Plaintiff and Class Members’ PII/PHI is private and sensitive in nature and was inadequately protected by Defendant. Defendant did not obtain Plaintiff and Class Members’ consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

60. As a direct and proximate result of Defendant’s wrongful actions and inaction and the resulting data breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to

---

<sup>26</sup> *Id.*

take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing “freezes” and “alerts” with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity. In particular, Plaintiff Kolka has already experienced signs of credit card fraud as following the data breach, he began to receive text messages from Capital One indicating that his PII had been used to open a fraudulent credit card account in his name.

61. Plaintiff and Class Members also lost the value of their PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

62. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including \$160.15 for online banking details, \$35.00 for credit reports, and \$62.61 for passports. Standalone Yahoo email accounts have been listed for as little as \$0.41, while banking logins are in the range of \$500, and verified Paypal accounts with high balances are listed at as much as \$2,000.

///

///

///

63. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	\$550
Auto insurance card:	\$70
AAA emergency road service membership card:	\$70
Wells Fargo bank statement:	\$25
Wells Fargo bank statement with transactions:	\$80
Rutgers State University student ID:	\$70

64. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. The improper disclosure and theft of their PII/PHI;
- b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;
- c. The untimely and inadequate notification of the data breach;
- d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and
- e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

//

//

### **CLASS ACTION ALLEGATIONS**

65. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rules 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

66. Plaintiff seeks to certify following Class, as defined below:

All persons in the United States whose PII and PHI was compromised by the data breach disclosed by Defendant John Fitzgibbon Memorial Hospital, Inc. on November 18, 2022.

67. Excluded from the Classes is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

68. *Numerosity.* The Members of the Classes are so numerous that joinder of all of them is impracticable. At this present moment, the Class is comprised of at least 112,702 individuals. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

69. *Commonality.* Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:



- a. Whether Defendant took reasonable steps and measures to safeguard Plaintiff' and Class Members' PII and PHI;
- b. Whether Defendant violated common and statutory regulations and requirements by failing to implement reasonable procedures and practices;
- c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;
- d. Whether Defendant knew or should have known about the data breach prior to the disclosure;
- e. Whether Defendant's acts or omissions described herein give rise to a claim of negligence;
- f. Whether Defendant had a duty to promptly notify Plaintiff and Class Members that their PII was, or potentially could be, compromised;
- g. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;
- h. The nature of the relief, including equitable relief, to which Plaintiff and the Class Members are entitled; and
- i. Whether Plaintiff and Class members are entitled to damages, civil penalties, and/or injunctive relief.

70. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiff' claims are typical of those of other Class Members because Plaintiff' PHI/PII, like that of every other Class Member, was collected by Defendant during its ordinary course of business and then subsequently misused and/or disclosed by Defendant.

71. *Adequacy of Representation.* Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiff intend to prosecute this action vigorously. Plaintiff claims are typical of the claims of other members of the Classes and Plaintiff have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiff and their counsel.

72. *Superiority of Class Action.* Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

73. *Superiority of Class Action.* Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

74. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

75. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

## **CAUSES OF ACTION**

### **FIRST CAUSE OF ACTION**

#### **Negligence**

76. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 75, inclusive, of this Complaint as if set forth fully herein.

77. Defendant requires any individual that uses its services to provide their PII and PHI to Defendant. Defendant collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

78. Defendant owed Plaintiff and the Class Members a duty of care in the handling of its patient's PII. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiff and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

79. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data security obligations.<sup>27</sup>

80. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.<sup>28</sup> NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

---

<sup>27</sup> Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> (last accessed January 16, 2022).

<sup>28</sup> "Framework for Improving Critical Infrastructure Cybersecurity," National Institute for Standards and Technology, <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf> (last accessed January 16, 2022).

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and

business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

81. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and the Class Members to provide reasonable security, including consistency

with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiff and the Class Members.

82. Defendant owed a duty to Plaintiff and the Class Members to design, maintain, and test their internal data systems to ensure that the PII/PHI in Defendant's possession was adequately secured and protected.

83. Defendant owed a duty to Plaintiff and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its custodianship, including adequately training its employees and others who accessed PII/PHI within its computer systems on how to adequately protect PII/PHI.

84. Defendant owed a duty to Plaintiff and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

85. Defendant owed a duty to Plaintiff and the Class Members to act upon data security warnings and alerts in a timely fashion.

86. Defendant owed a duty to Plaintiff and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiff and Class Members' decisions to entrust their PHI/PII to Defendants.

87. Defendant owed a duty to Plaintiff and the Class Members to disclose in a timely and accurate manner when data breaches occur.

88. Defendant owed a duty of care to Plaintiff and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems.



Defendant collected PII from Plaintiff and the Class Members. Defendants knew that a breach of its data systems would cause Plaintiff and the Class Members to incur damages.

89. Defendants breached its duties of care to safeguard and protect the PII/PHI which Plaintiff and the Class Members entrusted to it. Upon information and belief, Defendant adopted inadequate safeguards to protect the PII/PHI and failed to adopt industry-wide standards set forth above in its supposed protection of the PII/PHI. Defendant failed to design, maintain, and test its computer system to ensure that the PII/PHI was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach. Defendant's failure to implement reasonable and adequate safeguards to protect Plaintiff and Class Members' PII/PHI is evidenced in, *inter alia*, its unreasonably careless storage of password-protected files within the same folder as files containing the password to access those files.

90. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct

security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identify and address security gaps.

91. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

92. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiff and the Class members suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

93. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

## **SECOND CAUSE OF ACTION**

### **Breach of Implied Contract**

94. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 93, inclusive, of this Complaint as if set forth fully herein.

95. Plaintiff and Class Members entered into agreements for medical treatment with Defendant. In making those agreements, Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI to Defendant as requirement of receiving service. Plaintiff

and Class and Members accepted Defendant's offers and provided their PII and PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Defendant would implement reasonable and adequate data security to safeguard and protect the PII and PHI entrusted to them by Plaintiff and Class Members from unauthorized disclosure.

96. Thus, when Plaintiff and Class Members provided their PII and PHI to Defendant in exchange for medical services, they entered into implied contracts with Defendant under which Defendant agreed to and was obligated to reasonably protect their PII and PHI. Plaintiff and Class provided payment to Defendant, as well as their PII and PHI, under the reasonable but mistaken belief that any money they paid to Defendant in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI.

97. This implied contract is acknowledged and memorialized in Defendant's customer-facing documents, including, *inter alia*, Defendant's online Privacy Policy, which states:

“[w]e respect the confidentiality of your health information and recognize that information about your health is personal. We are committed to protecting your health information and to informing you of your rights regarding such information. We are also required by law to protect the privacy of your protected health information and to provide you with notice of these legal duties.”<sup>29</sup>

98. Defendant did not protect Plaintiff and Class Member's PII and PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under implied contract.

99. That Defendant would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiff and Class Members. Reasonable consumers value the privacy of their PII and PHI, and do not enter into agreements for medical

---

<sup>29</sup> “Notice of Privacy Practices” [https://www.fitzgibbon.org/Content/Uploads/fitzgibbon.org/files/Privacy%20Notice%20\(18x24%20poster\)%201-2023.pdf](https://www.fitzgibbon.org/Content/Uploads/fitzgibbon.org/files/Privacy%20Notice%20(18x24%20poster)%201-2023.pdf) (last accessed January 16, 2023).

services with healthcare providers which are known not to protect customer data. Accordingly, Plaintiff and Class Members would not have entered into agreements with Defendant and would not have provided them with their sensitive PII and PHI, had they known that Defendant would not implement such reasonable and adequate data security.

100. As a result of Defendant's breach, Plaintiff and Class Members have lost the benefit of their bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

101. Plaintiff and Class Members fully performed their obligations under the implied contract by providing their PII/PHI and making payments to Defendant.

102. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

### **THIRD CAUSE OF ACTION**

#### **Breach of Fiduciary Duty**

103. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 102, inclusive, of this Complaint as if set forth fully herein.

104. Plaintiff and Class Members provided their PII and PHI to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of

that information. Plaintiff and Class Members would not have provided Defendant with their PII and PHI had they known that Defendant would not take reasonable and adequate steps to protect it.

105. Defendant's acceptance and storage of Plaintiff; and Class Members' PII and PHI created a fiduciary relationship between Defendant and Plaintiff and Class Members. As a fiduciary of Plaintiff and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiff and Class Members' PII and PHI.

106. Defendant breached its fiduciary duties to Plaintiff and Class Members by, *inter alia*, failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security training for its employees, and otherwise failing to reasonably and adequately safeguard the PII and PHI of Plaintiff and Class Members.

107. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered damages. Plaintiff and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiff and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiff and Class Members of the data breach until weeks had passed. In addition, Plaintiff and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

108. Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

#### **FOURTH CAUSE OF ACTION**

##### **Quasi-Contract/Unjust Enrichment**

(On behalf of Plaintiff and the Nationwide Class)

109. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 108, inclusive, of this Complaint as if set forth fully herein.

110. Plaintiff and Class Members provided their PII and PHI and conferred a monetary benefit upon Defendant in exchange for healthcare services. Plaintiff and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII and PHI. Defendant was enriched when it sold its healthcare services at a higher price than it otherwise would have based on those reasonable but mistaken beliefs.

111. Defendant's enrichment came at the expense of Plaintiff and Class Members, who would not have paid for Defendant's services, or would have only been willing to paid substantially less for them, had they been aware that Defendant had not implement reasonable, adequate and statutorily mandated safeguards to protect their PII and PHI.

112. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members suffered have suffered damages in the form of their lost benefit of the bargains. Plaintiff and Class members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Defendant would not reasonably

and adequately protect their PII/PHI. Plaintiff and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

113. Defendant should not be permitted to retain Plaintiff' and Class Members' lost benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Defendant should not be allowed to benefit at the expense of consumers who trust Defendant to protect the PII and PHI that they are required to provide to Defendant in order to receive Defendant's services.

114. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

### **SIXTH CAUSE OF ACTION**

#### **Violation of the Missouri Merchandise Practices Act ("MMPA")**

##### **Mo. Rev. Stat. §§407.010, *et seq.***

115. Plaintiff repeats and incorporates herein by reference each and every allegation contained in paragraphs 1 through 114, inclusive, of this Complaint as if set forth fully herein.

116. Defendant is a "person" as defined under Mo. Rev. Stat. §407.010(5).

117. Defendant advertises, offers and sells "merchandise" as defined under Mo. Rev. Stat. §407.010(4), as it is engaged in the sale of services. In selling its services, Defendant engaged in trade or commerce as defined as defined under Mo. Rev. Stat. §407.010(6) and (7).



118. Plaintiff and Class Members purchased medical services from Defendant for personal, family, or household purposes.

119. Defendant engaged in “[t]he act, use or employment...of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce,” in violation of Mo. Rev. Stat. §407.020.

120. Specifically, Defendant engaged in misrepresentations and omissions of material fact when it represented to Plaintiff and Class Members that it would implement reasonable and adequate data security safeguards to protect their PII/PHI, when in fact it had not done so.

121. Defendant’s misrepresentations and omissions were material because they were likely to deceive reasonable consumers into entering agreements and providing their PII/PHI to Defendant. Plaintiff’s and Class Members would not have entered into agreements with Defendant and would not have provided Defendant with their PII/PHI had they known that Defendant would not protect their PII/PHI.

122. Plaintiff and Class Members have, at all times relevant to this action, acted as reasonable consumers in light of all circumstances.

123. As a direct and proximate result of Defendant’s unlawful, unfair, and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from the loss of their benefit of the bargain, loss of time spent dealing with the data breach, and the loss of the value of their PII/PHI. Plaintiff and Class Members seek all monetary and non-monetary relief allowable by law, including actual damages, punitive damages, attorney’s fees and costs, injunctive relief, and any other relief deemed just and proper.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

- a. For an Order certifying the Class as defined herein and appointing Plaintiff and their Counsel to represent the Class;
- b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff' and Class Members' PII/PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.
- d. For an award of actual damages and compensatory damages, in an amount to be determined at trial;
- e. For an award of punitive and treble damages, in an amount to be determined at trial;
- f. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and
- g. For such other and further relief as this Court may deem just and proper.
- h. Pre and post-judgment interest on any amounts awarded; and
- i. Such other and further relief as this court may deem just and proper.

## **DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: January 16, 2023

Respectfully Submitted by:

### **CASEY DEVOTI & BROCKLAND**

*/s/ Matthew J. Devoti*

---

Matthew J. Devoti #47751

Matthew C. Casey #49662

3201 Washington Avenue

St. Louis, Missouri 63103

(314) 421-0763

(314) 421-5059 Fax

mdevoti@caseydevoti.com

mcasey@caseydevoti.com

and

### **WILSHIRE LAW FIRM, PLC**

*/s/ Thiago M. Coelho*

---

Thiago M. Coelho\*

3055 Wilshire Blvd., FL 12

Los Angeles, CA 90010

Tel: (213) 381-9988

Fax: (213) 381-9989

thiago@wilshirelawfirm.com

*Attorneys for Plaintiff and the Proposed Class*

*\*Pro Hac Vice Forthcoming*